

FIGURATE PRIMES AND HILBERT'S 8TH PROBLEM

TIANXIN CAI, YONG ZHANG, AND ZHONGYAN SHEN

ABSTRACT. In this paper, by using the theory of elliptic curves, we discuss several Diophantine equations related with the so-called figurate primes. Meanwhile, we raise several conjectures related with figurate primes and Hilbert's 8th problem, including Goldbach's conjecture, twin primes conjecture and Catalan's conjecture as well.

1. FIGURATE PRIMES

In a letter to Crelle's Journal in 1844, Catalan stated that 8 and 9 are the only consecutive perfect powers, i.e., the Diophantine equation

$$p^a - q^b = 1$$

has unique positive integral solution $(p, q, a, b) = (2, 3, 3, 2)$. This is later known as Catalan's conjecture.

In 2004, P. Mihăilescu [4] proved this conjecture by making extensive use of the theory cyclotomic fields and Galois modules.

More generally, we have the Diophantine equation

$$(1.1) \quad p^a - q^b = k,$$

where p, q are primes, $a, b, k \in \mathbb{Z}^+$.

When $a = 1, q = 2, k = 1$, the solutions of (1.1) are exactly Fermat primes.

When $p = 2, b = 1, k = 1$, the solutions of (1.1) are exactly Mersenne primes.

When $a, b \geq 2, k = 1$, (1.1) is the Diophantine equation for Catalan's conjecture.

For $k > 1$, there are many authors who have investigated this problem, more information can be found in [3]: D9 Catalan conjecture & Difference of two powers and D10 Exponential diophantine equations.

When $a = b = 1, k = 2$, (1.1) is the Diophantine equation for twin primes conjecture.

In spring 2013, the first author [2] defined figurate primes as the positive binomial coefficients

$$\binom{p^a}{i}, \quad a \geq 1, \quad i \geq 1,$$

where p is a prime. The set includes all primes, but with the same density as the set of primes. We study the following Diophantine equation

$$(1.2) \quad \binom{p^a}{i} - \binom{q^b}{j} = k,$$

2000 *Mathematics Subject Classification.* Primary 11D41; Secondary 11G05.

Key words and phrases. figurate primes, elliptic curves, Goldbach's conjecture, Catalan's conjecture, linear Diophantine equations.

Project supported by the Natural Science Foundation of China (No. 11351002).

where p, q are primes, $a, b, i, j, k \in \mathbb{Z}^+$.

When $k = 1$, for $j = 1, i \geq 2$, we use elementary method to prove

Theorem 1.1. *For $(i, j) = (2, 1)$, (1.2) has exactly four solutions $(p, q, a, b) = (2, 5, 2, 1), (3, 2, 1, 1), (2, 3, 3, 3), (5, 3, 1, 2)$. For $(i, j) = (3, 1)$, (1.2) has exactly three solutions $(p, q, a, b) = (2, 3, 2, 1), (3, 83, 2, 1), (5, 3, 1, 2)$. For $(i, j) = (4, 1)$, (1.2) has exactly two solutions $(p, q, a, b) = (5, 2, 1, 2), (3, 5, 2, 3)$.*

For $i = b = 1, j = 2$. If a is even, it's easy to see that (1.2) has unique solution $(p, q) = (2, 3)$; if $a = 1$, it seems likely that (1.2) has infinitely many solutions, i.e., there are infinitely many pair of primes (p, q) satisfying

$$p - 1 = \binom{q}{2}.$$

However, it is even a harder problem than that of prime representations by binary forms. The least 10 examples are $(p, q) = (2, 2), (11, 5), (79, 13), (137, 17), (821, 41), (1831, 61), (3917, 89), (4657, 97), (5051, 101), (6329, 113)$; if $a > 1$ is odd, we guess that (1.2) has no solutions. It's true for $a = 3$ by an easy calculation.

Similarly, as the proof of Theorem 1, we can get that all the solutions of the Diophantine equation

$$p^a - 1 = \binom{q^b}{3}$$

are $(p, q, a, b) = (5, 2, 1, 2), (2, 3, 1, 1), (11, 5, 1, 1)$.

For $i = j \geq 2$, it's easy to verify that (1.2) has no solutions. By using the theory of elliptic curves, we have

Theorem 1.2. *For $(i, j) = (2, 3)$, (1.2) has unique solution $(p, q, a, b) = (3, 7, 2, 1)$; and for $(i, j) = (3, 2)$, (1.2) has exactly two solutions $(p, q, a, b) = (2, 3, 2, 1), (3, 7, 2, 1)$. For $(i, j) = (2, 4)$, (1.2) has exactly two solutions $(p, q, a, b) = (2, 5, 2, 1), (3, 7, 2, 1)$; and for $(i, j) = (4, 2)$, (1.2) has no solutions.*

When $k = 2$, we have

Theorem 1.3. *For $(i, j) = (2, 3)$, (1.2) has exactly two solutions $(p, q, a, b) = (2, 2, 2, 2), (3, 3, 1, 1)$; and for $(i, j) = (3, 2)$, (1.2) has no solutions. For $(i, j) = (2, 4)$, (1.2) has unique solutions $(p, q, a, b) = (3, 2, 1, 2)$; and for $(i, j) = (4, 2)$, (1.2) has unique solution $(p, q, a, b) = (5, 3, 1, 1)$.*

2. HILBERT'S 8TH PROBLEM

Among the 23 problems that David Hilbert raised at the International Congress of Mathematicians in Paris in 1900, the 8th one might be the most profound and difficult, it includes Riemann Hypothesis, Goldbach's conjecture and twin primes conjecture.

Goldbach's conjecture (1742) is one of the most important unsolved problems in number theory:

Every even integer greater than 2 can be expressed as the sum of two primes, i.e.,

$$n = p + q, \quad n \geq 4,$$

where n is even and p, q are primes. And every odd integer greater than 5 can be expressed as the sum of three primes, i.e.,

$$n = p + q + r, \quad n \geq 7,$$

where n is odd and p, q, r are primes. The first half for even number is still an open problem.

However, by fundamental theorem of arithmetic, each positive integer can be constructed from the product of primes, prime numbers are the basic building blocks of any positive integer in multiplication. Meanwhile, it seems that primes don't play key role in addition. Besides, it's not a perfect result that each even integer is the sum of two primes while each odd integer is the sum of three primes, according to Goldbach's conjecture.

What we have to point out is that, among the composites in figurate primes the amounts of even integers is as many as those of odd integers, they are many more than powers of 2, cf. [3]: A19 Values of n making $n - 2^k$ prime & Odd numbers not of the form $\pm p^a \pm 2^b$. By calculations with computer, we check and find that every positive integer $1 < n \leq 10^7$ can be expressed as the sum of two figurate primes, i.e., the Diophantine equation

$$(2.1) \quad n = \binom{p^a}{i} + \binom{q^b}{j}$$

always has solutions with primes p, q and $a, b, i, j \in \mathbb{Z}^+$. Therefore, we raise the following

Conjecture 2.1. *Every positive integer $n > 1$ can be expressed as the sum of two figurate primes.*

Conjecture 2.2. *(weak twin primes conjecture) There are infinitely many pairs of figurate primes with difference 2.*

Moreover, we read Hilbert's speech carefully, in the statement of the 8th problem he mentioned

"After an exhaustive discussion of Riemann's prime number formula, perhaps we may sometime be in a position to attempt the rigorous solution of Goldbach's problem, viz., whether every integer is expressible as the sum of two positive prime numbers; and further to attack the well-known question, whether there are an infinite number of pairs of prime numbers with the difference 2, or even the more general problem, whether the linear diophantine equation

$$ax + by + c = 0$$

(with given integral coefficients each prime to the others) is always solvable in prime numbers x and y ."

With the idea of figurate primes and by numerical calculations, we have

Conjecture 2.3. *For any positive integers a and b , $(a, b) = 1$, when $n \geq (a - 1)(b - 1)$, there always exists prime pair (x, y) , such that*

$$ax + by = n.$$

Meanwhile, if we call a positive integer n a proper one if n is a figurate prime but not a prime. Then we even have a stronger

Conjecture 2.4. *Every positive integer $n > 5$ can be expressed as the sum of a prime and a proper figurate prime.*

3. PROOF OF THE THEOREMS

Proof of Theorem 1.1. When $k = 1$, for $(i, j) = (2, 1)$, (1.2) is equal to

$$(p^a + 1)(p^a - 2) = 2q^b.$$

Clearly, $d = (p^a + 1, p^a - 2) = 1$ or 3 .

If $d = 1, p = 2$, we have

$$2^a - 2 = 2, 2^a + 1 = q^b$$

or

$$2^a - 2 = 2q^b, 2^a + 1 = 1,$$

it's easy to see that $(p, q, a, b) = (2, 5, 2, 1)$.

If $d = 1, p > 2$, we have

$$p^a - 2 = q^b, p^a + 1 = 2$$

or

$$p^a - 2 = 1, p^a + 1 = 2q^b,$$

it's easy to see that $(p, q, a, b) = (3, 2, 1, 1)$.

If $d = 3$, then $q = 3$. For $p = 2$, we have

$$2^a - 2 = 6, 2^a + 1 = 3^{b-1}$$

or

$$2^a - 2 = 2 \cdot 3^{b-1}, 2^a + 1 = 3,$$

it's easy to see that $(p, q, a, b) = (2, 3, 3, 3)$.

For $p > 2$, we have

$$p^a - 2 = 3, p^a + 1 = 2 \cdot 3^{b-1}$$

or

$$p^a - 2 = 3^{b-1}, p^a + 1 = 6,$$

it's easy to see that $(p, q, a, b) = (5, 3, 1, 2)$.

As for the cases $(i, j) = (3, 1)$ or $(4, 1)$, we can prove by using similar method. \square

Proof of Theorem 1.2. When $k = 1$, for convenience, put $p^a = y, q^b = x$ for $(i, j) = (2, 3)$ and $p^a = x, q^b = y$ for $(i, j) = (3, 2)$ in (1.2), respectively. Let

$$x = \frac{X + 12}{12}, y = \frac{Y + 36}{72},$$

the converse transformation is

$$X = 12x - 12, Y = 36(2y - 1).$$

Then, we have

$$Y^2 = X^3 - 144X + 11664, Y^2 = X^3 - 144X - 3024,$$

respectively.

Using **Magma**, we get all the integral points on the above two elliptic curves. For $Y^2 = X^3 - 144X + 11664$, the point $(X, Y) = (72, 612)$ leads to the unique solution $(p, q, a, b) = (3, 7, 2, 1)$ of (1.2). For $Y^2 = X^3 - 144X - 3024$, the points $(X, Y) =$

$(36, 180), (84, 756)$ lead to the two solutions $(p, q, a, b) = (2, 3, 2, 1), (3, 7, 2, 1)$ of (1.2).

Let $p^a = y, q^b = x$ for $(i, j) = (2, 4)$ in (1.2), let

$$x = \frac{X+3}{6}, \quad y = Y+2,$$

we have

$$Y^2 = 3X^4 + 6X^3 - 3X^2 - 6X + 81.$$

Using **Magma**, we get all the integral points on this elliptic curve, they are

$$(X, \pm Y) = (10, -11; 189), (-1, -2, 1, 0; 9), (-4, 3; -21), (-6, 5; 51), (-92, 91; 14499),$$

by some calculations, we find that $(X, Y) = (3, 21), (5, 51)$ lead to the two solutions $(p, q, a, b) = (2, 5, 2, 1), (3, 7, 2, 1)$ of (1.2).

Let $p^a = x, q^b = y$ for $(i, j) = (4, 2)$ in (1.2), let

$$x = \frac{X+3}{6}, \quad y = Y+2,$$

we have

$$Y^2 = 3X^4 + 6X^3 - 3X^2 - 6X - 63.$$

Using **Magma**, we get all the integral points on this elliptic curve, which are

$$(X, \pm Y) = (-3, 2; 3),$$

it's easy to see that there are no solutions for $(i, j) = (4, 2)$. □

Proof of Theorem 1.3. When $k = 2$, for convenience, put $p^a = y, q^b = x$ for $(i, j) = (2, 3), k = 2$ and $p^a = x, q^b = y$ for $(i, j) = (3, 2), k = 2$ in (1.2), respectively. Let

$$x = \frac{X+12}{12}, \quad y = \frac{Y+36}{72},$$

the converse transformation is

$$X = 12x - 12, \quad Y = 36(2y - 1).$$

Then, we have

$$Y^2 = X^3 - 144X + 22032, \quad Y^2 = X^3 - 144X - 19440,$$

respectively.

Using **Magma**, we get all the integral points on the above two elliptic curves. For $Y^2 = X^3 - 144X + 22032$, the points $(X, Y) = (36, 252), (24, 180)$ lead to the solutions $(p, q, a, b) = (2, 2, 2, 2), (3, 3, 1, 1)$ of (1.2). And $Y^2 = X^3 - 144X - 19440$ has no integral points, hence (1.2) has no solutions for $(i, j) = (3, 2)$.

Let $p^a = y, q^b = x$ for $(i, j) = (2, 4), k = 2$ in (1.2), let

$$x = X, \quad y = \frac{Y+3}{6},$$

we have

$$Y^2 = 3X^4 - 18X^3 + 33X^2 - 18X + 153.$$

Using **Magma**, we get all the integral points on this elliptic curve, which are

$$(X, \pm Y) = (-1, 4; 15),$$

by some calculations, we find that $(X, Y) = (4, 15)$ lead to the unique solutions $(p, q, a, b) = (3, 2, 1, 2)$ of (1.2).

Let $p^a = x, q^b = y$ for $(i, j) = (4, 2), k = 2$ in (1.2), let

$$x = X, y = \frac{Y+3}{6},$$

we have

$$Y^2 = 3X^4 - 18X^3 + 33X^2 - 18X - 135.$$

Using **Magma**, we get all the integral points on this elliptic curve, which are

$$(X, \pm Y) = (-2, 5; 15),$$

by some calculations, we find that $(X, Y) = (5, 15)$ lead to the unique solution $(p, q, a, b) = (5, 3, 1, 1)$ of (1.2). \square

In figure 1, we display the graph of the quartic curve

$$Y^2 = 3X^4 - 18X^3 + 33X^2 - 18X - 135.$$

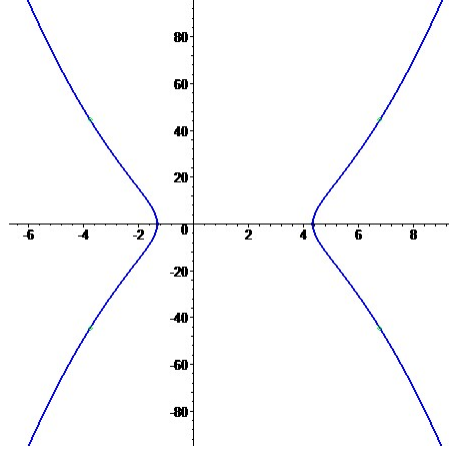


FIGURE 1. $Y^2 = 3X^4 - 18X^3 + 33X^2 - 18X - 135$

4. TWO CONJECTURES RELATED WITH CATALAN EQUATION

In [1], the first author raised a new variant of the Hilbert-Waring problem: to express a positive integer n as the sum of s positive integers whose product is a k -th power, i.e.,

$$n = x_1 + x_2 + \cdots + x_s$$

such that

$$x_1 x_2 \cdots x_s = x^k,$$

for $n, x_i, x, k \in \mathbb{Z}^+$, which may be regarded as a generalization of Waring's problem:

$$n = x_1^k + x_2^k + \cdots + x_s^k.$$

Now we expand this idea to Catalan's equation. Let's consider

$$(4.1) \quad \begin{cases} A - B = 1, \\ AB \text{ is square-full}, \end{cases}$$

where A, B are positive integers.

This is a generalization of Catalan equation. By using the method of Pell's equation, it's easy to show that there are infinitely many solutions of (4.1), the least three are $(8, 9), (288, 289), (675, 676)$.

However, after calculations with computer, we find and raise the following conjectures (we have checked up to $B < A < 10^6$)

Conjecture 4.1. *Let $r \geq 0$ be integer, the Diophantine equation*

$$\begin{cases} A - B = 2^r, \\ AB \text{ is cube-full,} \end{cases}$$

has no solutions for $r = 0$, and has unique solution $(A, B) = (2^{r+1}, 2^r)$ for $r \geq 1$.

Moreover, we have

Conjecture 4.2. *Let $r \geq 1$ be integer, there are infinitely many prime p such that the Diophantine equation*

$$(4.2) \quad \begin{cases} A - B = p, \\ AB \text{ is cube-full,} \end{cases}$$

has no solutions. Moreover, the least prime is 29.

It's easy to verify that for every integer $2 \leq n \leq 28$, (4.2) has solutions. However, we even don't know if there is a solution for infinitely many prime p .

5. ACKNOWLEDGEMENTS

The authors wish to thank Dr. Deyi Chen and Mr. Tanyue Gao for their kind help in calculation, especially in verifying Conjectures 2.1, 4.1 and 4.2.

REFERENCES

1. T. Cai and D. Chen, A new variant of the Hilbert-Waring problem, *Math. Comp.* **82** (2013), no. 284, 2333–2341.
2. T. Cai, *The Book of Numbers*, High Education Press, Beijing, 2014.
3. R. K. Guy, *Unsolved Problems in Number Theory*, 3rd edition, Springer, 2004.
4. P. Mihăilescu, Primary cyclotomic units and a proof of Catalan's conjecture, *J. reine angew. Math.* 572 (2004), 167–195.

DEPARTMENT OF MATHEMATICS, ZHEJIANG UNIVERSITY, HANGZHOU, 310027, PEOPLE'S REPUBLIC OF CHINA

E-mail address: txcai@zju.edu.cn

DEPARTMENT OF MATHEMATICS, ZHEJIANG UNIVERSITY, HANGZHOU, 310027, PEOPLE'S REPUBLIC OF CHINA

E-mail address: zhangyongzju@163.com

DEPARTMENT OF MATHEMATICS, ZHEJIANG INTERNATIONAL STUDY UNIVERSITY, HANGZHOU, 310012, PEOPLE'S REPUBLIC OF CHINA

E-mail address: huanchenszhan@yahoo.com.cn